Best Practices for Protecting Your Personal Information from Hackers

From the most senior executive to the most junior intern, employees are leveraging advanced interconnected technologies in new ways in their personal life. This introduces new risks to their privacy and at times, new risks to their employer. In most cases, it is in the best interests of employers to help employees understand how to better protect their personal information.

Every home IT configuration will be different and it can be challenging for a company to provide useful, actionable guidance to every employee. We have found that the most important recommendation is to encourage employees to adopt an attitude of personal responsibility and continuous questioning regarding optimal home security configuration.

We also recommend employees leverage the following actions to reduce risks to their home technology:

- Use two-factor or multi-factor authentication for every account, including every cloud service or email account that you use at home. This is one of the most important things that you can do to mitigate risks. If an account does not offer multi-factor authentication, consider closing it.
- Update and patch operating systems, applications and anti-virus/anti-malware software. This reduces multiple risks.
- Use a reputable password manager like Dashlane or Lastpass. This will help you keep all of your passwords up to date and secure and generally make life easier.
- Change the default password on every device you own, including connected “Internet of Things” devices such as security cameras, baby monitors, and thermostats, as well as tablets, smart TVs, laptops, and PCs.
- Use a managed DNS service from Google, Verisign, or OpenDNS to help prevent accidental navigation to websites that have been taken over by malicious actors and help stop communications from malicious code in home systems (including IoT devices) to malicious control sites.
- Stay informed of the dynamic cyber threat and increase your awareness of adversary capabilities. This will help you better defend your systems at home and help you make better decisions at work. See our Threat Brief at ThreatBrief.com for actionable insights for businesses, governments, and home users.

All questions and enquiries regarding this white paper should be directed to:
Bob Gourley
Partner and Co-Founder
Bob.gourley@cognitiocorp.com

Cognitio Cyber Leadership

Cognitio is a strategic consulting and engineering firm enabling companies to more effectively maximize the impact of technology investments and reduce overall digital risk. Cognitio helps clients improve their defenses by:

- Independent assessments of security posture leveraging best practices and our Cyber360 framework
- Providing executive-level “CISO-as-a-Service” support
- Campaign plans and technology assessments enabling optimization of security spend

Roger Hockenberry

CEO, Cognitio

Background in cyber security in the IT and Healthcare industries and in the Intelligence Community.

Bob Gourley

Partner, Cognitio

DoD and Intelligence background. Cyber Intelligence assessments across multiple industries.

David Highnote

Partner, Cognitio

Background in strategic consulting and cyber assessments in multiple industries. Media experience.

Bob Flores

Partner, Cognitio

Former CIA CTO. Background in enterprise tech and cyber security assessments.

Chris Ward

Senior Analyst, Cognitio

DoD and consulting background. Strong in enterprise IT including applying right tech to mission needs.

Chuck Hall

COO, Cognitio

Background in Healthcare IT and cybersecurity as well as business leadership.

Crystal Lister

Lead Analyst, Cognitio

Background in all-source cyber threat and counterintelligence analysis in the Intelligence Community.

Cognitio analysts include Dan Cybulski, former head of high performance computing for the U.S. government, and Leslie Wilfong, highly regarded data scientist.

CognitioCorp.com